UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,423	03/29/2001	Michael S. Ripley	42390P10855	9405

8791 7590 08/02/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
HAMILTON, MONPLAISIR G	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 08/02/2004

10

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/823,423	Applicant(s) RIPLEY ET AL.
	Examiner Monplaisir G Hamilton	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 remain for examination.

Response to Arguments

2. Applicant's arguments, see Paper No. 9, filed 5/03/04, with respect to the rejection(s)of Claim(s) 1-4, 6-9, 11-19 and 21-26 under 35 U.S.C. § 102(a) as being anticipated by *Content Protection for Recordable Media Specification* Revision 0.94 by IBM et al, Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by US 6289102 issued to Ueda et al, herein referred to as Ueda and Claims 5, 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Content Protection for Recordable Media Specification Revision .94 by IBM et al, herein referred to as IBM in view of US 5949881 issued to Davis, herein referred to as Davis, have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Lotspiech (US 6,748,539).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 3 and 4 recites the limitation "the at least one". There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim Objections

4. Claims 5, 12 and 20 is objected to because of the following informalities: "used by said encryption subsystem to **encrypted** said data". Encrypted should be encrypt, appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-9, 11-14, 16, 18-21, 23-24, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Lotspiech (US 6,748,539).

Referring to Claim 1:

Lotspiech discloses a system comprising:

a number generator to generate a nonce (col 5, lines 20-30); and

an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus (col 3, lines 10-16), wherein said encryption bus key is derived based on [1] a portion of the key distribution data block, [2]a device key assigned to said encryption subsystem and [3]the nonce generated by the number generator (col 3, lines 10-20; col 4, line 65-col 5, line 10).

Referring to Claim 11:

Lotspiech discloses a method comprising:

a storage device reading a key distribution data block from a storage medium (col 4, line 65-col 5, line 10);

the storage device processing at least a portion of said key distribution data block using least one device key to compute a media key (col 5, lines 1-10);

the storage device fetching a nonce generated by a number generator (col 5, lines 1-6, 20-25);

the storage device combining said nonce with said media key using a one-way function to generate a bus key (col 5, lines 5-10);

the storage device encrypting data read from the storage medium using the bus key generated by the storage device (col 5, lines 5-10); and

the storage device transmitting the encrypted data over a data bus to a host device (col 5, lines 5-20).

Referring to Claim 18:

Lotspiech discloses an apparatus comprising:

a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic (col 5, lines 1-10),

a one-way function and an encryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key (col 5, lines 1-5),

said one-way function combines said media key with a nonce generated by a number generator to produce a bus key (col 5, lines 1-10, 20-25) and

said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus to a host device (col 5, lines 5-25).

Referring to Claim 2:

Lotspiech discloses the limitations of Claim 1 above. Lotspiech further discloses a decryption subsystem coupled to said data bus to, decrypt said encrypted data received over the data bus using a decryption bus key derived based [1] a portion of the key distribution data block, [2] a device key assigned to said decryption subsystem and [3] the nonce generated by the number generator (col 5, lines 10-20).

Referring to Claim 3:

Lotspiech discloses the limitations of Claim 1 above. Lotspiech further discloses said encryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key (col 5, lines 1-10);

a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator (col 5, lines 1-6);

and an encryption logic to encrypt data accessed from said storage medium using said encryption bus key (col 5, lines 1-10).

Referring to Claim 4:

Lotspiech discloses the limitations of Claim 2 above. Lotspiech further discloses said decryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key (col 5, lines 10-20);

a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator (col 5, lines 15-20); and

a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key (col 5, lines 18-20).

Referring to Claims 5, 12 and 20:

Lotspiech discloses the limitations of Claims 1, 11 and 18 above. Lotspiech further discloses said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus (col 5, lines 20-35).

Referring to Claims 6, 16 and 26:

Lotspiech discloses the limitations of Claims 2, 11 and 19 above. Lotspiech further discloses said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (col 4, lines 20-30).

Referring to Claim 7:

Lotspiech discloses the limitations of Claim 2 above. Lotspiech further discloses said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device (col 5, lines 1-20; Fig. 1).

Referring to Claim 8:

Lotspiech discloses the limitations of Claim 2 above. Lotspiech further discloses said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised (col 5, lines 10-20).

Referring to Claim 9:

Lotspiech discloses the limitations of Claim 2 above. Lotspiech further discloses wherein said storage medium is selected from digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory magnetic card and optical card (Fig. 1).

Referring to Claim 13:

Lotspiech discloses the limitations of Claim 11 above. Lotspiech further discloses decrypting the encrypted data received over the data bus (col 5, lines 10-20).

Referring to Claim 14:

Lotspiech discloses the limitations of Claim 13 above. Lotspiech further discloses said decrypting the encrypted data received over the data bus comprises:

a host device reading the key distribution data block from the storage medium (col 5, lines 10-20);

the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key (col 5, lines 10-20);

the host device fetching the nonce generated by the number generator (col 5, lines 10-35);

the host device combining said media key with the nonce using a one-way function to generate a bus key (col 5, lines 10-20); and

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device (col 5, lines 10-20).

Referring to Claim 19:

Lotspiech discloses the limitations of Claim 18 above. Lotspiech further discloses a host device coupled to said storage device via said data bus, said host device including

a processing logic, a one-way function and a decryption logic (col 5, lines 10-20), wherein said processing logic processes at least a portion of said key distribution data block

using a device key assigned to said host device to compute a media key (col 5, lines 10-20), said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key (col 5, lines 10-35).

Referring to Claim 21:

Lotspiech discloses the limitations of Claim 19 above. Lotspiech further discloses said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised (col 5, lines 10-20).

Referring to Claim 23:

Lotspiech discloses the limitations of Claim 19 above. Lotspiech further discloses said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer (col 1, line 30-35; Fig. 1).

Referring to Claim 24:

Lotspiech discloses the limitations of Claim 19 above. Lotspiech further discloses said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card (Fig. 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 10, 17 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (US 6,748,539) in view of Kato et al (US 6,751,321).

Referring to Claims 10, 17 and 22:

Lotspiech discloses the limitations of Claims 2, 14 and 19 above.

Lotspiech does not explicitly disclose "said number generator is a random number generator residing within the host device".

Kato discloses said number generator is a random number generator residing within the host device (col 5, lines 30-50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that the "media id" number generator that produces the nonce is a random number generator. One of ordinary skill in the art would have been motivated to do this because it would provide increased security (col 5, lines 47-50).

7. Claims 15 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (US 6,748,539) in view of Nagai et al. (US 2002/0015494).

Referring to Claim 15:

Lotspiech discloses the limitations of Claim 13 above.

Lotspiech does not explicitly disclose "the host device requesting a descramble key required for descrambling scrambled content from said storage device;

the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device;

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device the host device descrambling said decrypted data using said descramble key decrypted by said host device."

Nagai disclose the host device requesting a descramble key required for descrambling scrambled content from said storage device (paragraph 0059);

the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device (paragraph 0055);

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device the host device descrambling said decrypted data using said descramble key decrypted by said host device (paragraphs 0051 and 0059-0060),

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Lotspiech such that the data stored on the storage medium is scrambled. One of ordinary skill in the art would have been motivated to do this because it would provide a higher level of copy protection (paragraphs 0049-0051).

Referring to Claim 25:

Lotspiech discloses the limitations of Claim 19 above.

Lotspiech does not explicitly disclose "said storage medium is embodied in the form of a DVD containing scrambled content".

Nagai disclose said storage medium is embodied in the form of a DVD containing scrambled content (paragraph 0059).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that the information stored on the medium is scrambled. One of ordinary skill in the art would have been motivated to do this because it would provide a higher level of copy protection (paragraphs 0049-0051).

Final Rejection

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Specifically applicant's amendment to include transmitting to a host device and to overcome the 35 U.S.C § 112 rejection regarding the ambiguity presented when deriving the bus key in the originally filed claims. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100